

SureVote

David Chaum

Dr. Chaum is widely recognized as the inventor of electronic cash called eCash and also as the founder of DigiCash, the pioneering electronic cash company. He has published over 50 original scientific articles on cryptography and has been awarded more than twenty patents in the field. Chaum is also known in voting circles for publishing in 1981, while a graduate student at Berkeley, a paper presenting for the first time ways to secure and protect privacy of elections conducted over computer networks. Most of the subsequent scientific results, trials, and other products for secure Internet voting can be traced to his seminal work. Chaum originally developed the SureVote paradigm in early 2000 for use in emerging countries where elections are often overturned after their integrity is called into question. After the US election in November 2000, Chaum adapted the approach and founded SureVote.

Mr. Chairman, members of the Committee,

Let me begin with some basic facts about election technology.

The “gold standard” against which all election technology should be judged, as far as integrity and privacy, is the traditional: special printed ballots that are marked by voters in booths, placed in boxes, and later counted by hand, with observers/poll-workers from all major parties keeping a close eye on the ballots—or the boxes containing them—at each stage.

All current election technology that includes electronics falls way short of this mark, because observers cannot do their job. The reason is that only the maker of the “electronic ballot boxes” used can have any confidence in what can happen to the electronic representation of the ballots it stores. (Has the box, for example, been deliberately but undetectably caused to swap votes between candidates, or has it been designed to invade privacy by somehow revealing the time at which certain votes were cast.)

There is, however, a different paradigm for electronic elections, and its superiority and suitability is something that has been known to and proven by the federal government for years (though arguably only in parts).

When Treasury wants the public to trust something, it prints it on special paper. (For instance, serial numbers are put on banknotes in a single room with galleries that are open to the public). Faith in money is not unlike confidence in elections.

When Defense wants to secure transmission of important choices made at a remote locations, it prints codes on paper, distributes them in (special) envelopes, and when any such “launch code” is received, the missile fires to the location corresponding to that particular code.

When federal regulators want to leave implementation to states, but ensure a high level is applied uniformly, they simply require adherence to strict federal standards. For instance, we now have a “national identity card” ...although nobody calls it that. The trick is that it is implemented by each state “independently” adhering to high federal standards for driver/identity cards.

All these proven techniques can be combined to make a system with integrity and privacy that matches (and even betters) that of the gold-standard paper-ballot. Its ballots (or security strips) are printed at a central location with two “PIN” codes for each candidate. A voter (in effect) provides the first code for a candidate by phone, web or whatever means and it is routed to a set of data centers. Each data center is run by a different part of government or major party—just like the observers/poll-workers in the gold standard. These centers must cooperate (and cannot cheat unless they all collude) to recognize the code as valid and compute the second code, which they send back to the voter. This second code acts as a strong confirmation to the voter who checks that it matches that printed next to their candidate. Only after voting is over, do the datacenters work together to shuffle the digital ballots and then reveal their content.

My overall recommendation? Again based on best practices, is a competition between consortia proposing different solutions (hopefully some of which will include the new paradigm I sketched). A consortium should be able to include government laboratories or agencies as well companies and universities. The federal government defines the rules: qualifying requirements, functions to be provided and deadlines for each stage. I envision a “voting proving ground,” where each system is used in mock elections by paid members of the public, like in a survey, and also studied by experts with full access to the implementation. At the end, a panel of experts from federal agencies decides which systems are acceptable and criteria for federal elections are formed around them.